

DESAIN DAN IMPLEMENTASI METODE SELF ENCRYPTION PADA PENGAMANAN FILE

MOCH REZKY DEBBY RAHARDJO

(Pembimbing : Dr. Guruh Fajar Shidik, S.kom., M.Cs)

Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro

www.dinus.ac.id

Email : 111201206590@mhs.dinus.ac.id

ABSTRAK

Kebijakan Bring Your Own Device (BYOD) membuat orang-orang menyimpan data-data pada satu perangkat. Ditambah dengan semakin lebarnya jaringan nirkabel, akses menuju layanan cloud storage menjadi semakin mudah. Namun proses pengunggahan data ke cloud storage yang terbuka tanpa enkripsi, memungkinkan data tersebut jatuh ke tangan orang lain. Hal ini juga dapat terjadi saat data sudah berada dalam cloud storage. Untuk itu diperlukan pengamana tambahan sebelum data diunggah ke cloud storage maupun data yang hanya akan disimpan di media penyimpanan lokal. Dengan mengimplementasikan algoritma Self-Encryption, aplikasi yang dibuat pada penelitian ini dapat mengenkripsi file dengan berbagai jenis ekstensi dengan berbagai macam ukuran. Dari hasil implementasi dan pengujian, didapatkan hasil pengujian berupa waktu proses enkripsi dan dekripsi dari 12 data yang diuji dan ketahanan dari kunci yang terbentuk pada proses enkripsi dari 12 data uji. Semakin besar ukuran filenya, maka semakin lama waktu yang dibutuhkan untuk enkripsi dan dekripsi, serta semakin besar pula nilai entropi dari kunci yang terbentuk. Serta aplikasi ini memiliki kemampuan pengelolaan kunci yang memudahkan pengguna untuk melakukan dekripsi.

Kata Kunci : algortima Self-Encryption, kriptografi, kamanan data

DESIGN AND IMPLEMENTATION OF SELF ENCRYPTION METHOD ON FILE SECURITY

MOCH REZKY DEBBY RAHARDJO

(Lecturer : Dr. Guruh Fajar Shidik, S.kom., M.Cs)

*Bachelor of Informatics Engineering - S1, Faculty of Computer
Science, DINUS University*

www.dinus.ac.id

Email : 111201206590@mhs.dinus.ac.id

ABSTRACT

Bring Your Own Device Policy (BYOD) keeps people storing data on one device. Coupled with the growing width of wireless networks, access to cloud storage services becomes even easier. But the process of uploading data to open cloud storage without encryption, allowing the data to fall into the hands of others. This can also happen when data is already in cloud storage. This requires additional precedence before data is uploaded to cloud storage or data that will only be stored in local storage media. By implementing the Self-Encryption algorithm, the applications created in this study can encrypt files with different types of extensions with different sizes. From the results of implementation and testing, obtained the test results in the form of encryption and decryption process of the 12 data tested and the resistance of the key formed by the encryption process of 12 test data. The larger the file size, the longer it takes for encryption and decryption, and the greater the entropy value of the key that is formed. And this application has a key management capability that allows users to do the decryption.

Keyword : Self-Encryption algorithm, cryptography, data security